Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR05/000615

International filing date: 04 March 2005 (04.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2004-0015162
Filing date: 05 March 2004 (05.03.2004)

Date of receipt at the International Bureau: 17 May 2005 (17.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office

출 원 번 호 : 특허출원 2004년 제 0015162 호
Application Number 10-2004-0015162

출 원 일 자 : 2004년 03월 05일
Date of Application MAR 05, 2004

출 원 인 : 삼성전자주식회사 외 5 명
Applicant(s) SAMSUNG ELECTRONICS CO., LTD., et al

2005 년 04 월 07 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2004.03.05

【발명의 국문명칭】 무선 휴대 인터넷 시스템에서 멀티 캐스트 서비스용 트래픽 암호화 관리 방법

【발명의 영문명칭】 Method for managing traffic encryption key for the multicast services in the wireless potable internet system

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【명칭】 유미특허법인

【대리인코드】 9-2001-100003-6

【지정된변리사】 이원일

【포괄위임등록번호】 2001-038431-4

【발명자】

【성명의 국문표기】 조석헌

【성명의 영문표기】 CHO,SEOK HEON

【주민등록번호】 770127-1543416

【우편번호】 570-976

【주소】 전라북도 익산시 신동 775-21번지

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 유미특허법인 (인)

【수수료】

【기본출원료】	30	면	38,000 원
【가산출원료】	0	면	0 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	38,000 원		
【감면사유】	정부출연연구기관		
【감면후 수수료】	19,000 원		

【기술이전】

【기술양도】	희망
【실시권허여】	희망
【기술지도】	희망

【요약서】

【요약】

IEEE 802.16 WirelessMAN기반의 무선 인터넷 시스템에서는 서비스를 안전하게 제공하기 위하여 트래픽 데이터에 대한 암호화 기능을 정의하고 있다. 트래픽 데이터에 대한 암호화 기능은 서비스의 안정성 및 망의 안정성을 위하여 필요한 기본적인 요구사항으로 대두되고 있다. IEEE 802.16 WirelessMAN 시스템에서는 이와 같은 트래픽 데이터의 암호화 및 복호화를 위하여 단말 (SS)과 기지국 (BS) 사이에 보안 키 관리 프로토콜 (PKM: Privacy Key Management) MAC 메시지들을 정의하고 있다.

본 발명은 IEEE 802.16 WirelessMAN 시스템에서 정의하고 있는 트래픽 데이터에 대한 암호화 키를 관리하는 방법에 있어서, 암호화 키들에 대한 생성, 분배 및 갱신하는 방법을 정의하기 위한 것이다. 특히, IEEE 802.16 WirelessMAN 시스템에서는 Multicast 서비스와 Broadcast 서비스용 암호화 키 갱신 및 분배 방법에 대하여 Unicast 서비스용 암호화 키 갱신 및 분배하는 방법과 동일하게 고려하고 있다. 이에 본 발명은 Multicast 서비스와 Broadcast 서비스용 암호화 키들을 보다 효율적으로 관리하기 위해서 Unicast 서비스용 암호화 키를 관리하는 방법과는 다른 방법을 제시한다. 본 발명의 결과로써 IEEE 802.16 WirelessMAN 시스템은 트래픽 데이터에 대한 암호화 키를 보다 효과적이고 유연하게 관리할 수 있게 된다.

【대표도】

도 2

【색인어】

IEEE 802.16 WirelessMAN, 트래픽 암호화 키 (TEK), 갱신

【명세서】

【발명의 명칭】

무선 휴대 인터넷 시스템에서 멀티 캐스트 서비스용 트래픽 암호화 관리 방법{Method for managing traffic encryption key for the multicast services in the wireless potable internet system}

【도면의 간단한 설명】

<1> 도 1은 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 생성, 분배 및 갱신하는 절차도

<2> 도 2는 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 갱신하는 방법도

<3> 도 3은 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 갱신 절차도,

<4> 도 4는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 갱신 방법도,

<5> 도 5은 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신하기 위한 추가 PKM 파라미터 테이블,

<6> 도 6은 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 분배시 MAC Header의 CID값과 트래픽 암호화 키를 암호화하는 입력 키간의 관계도.

<7> 도 7은 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 분배하는 방식에서의 트래픽 암호화 키 상태 머신 흐름도.

<8> 도 8은 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 분배하는 방식에서의 트래픽 암호화 키 상태 천이 테이블.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명의 목적은 IEEE 802.16 WirelessMAN 시스템 기반의 무선 인터넷 시스템에서 Multicast 서비스용 또는 Broadcast 서비스용 트래픽에 대한 암호화 키를 관리하는 방법을 제안한다.

<10> 본 발명의 결과로써, 해당 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 (TEK : Traffic Encryption Key)를 갱신 및 분배하는데 있어서 무선 구간 신호 채널의 사용 부하를 감소시킬 수 있다. 즉, Multicast 서비스나 Broadcast 서비스를 제공받고 있는 모든 가입자들이 트래픽 암호화 키 갱신 요청을 하고 이에 대하여 기지국이 동일한 트래픽 암호화 키를 모든 가입자들에게 개별적으로 응답을 하는 방법 대신에 기지국이 내부 이벤트로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하고 이를 방송 채널을 통하여 모든 가입자들에게 동시에 분배하는 방법을 채택함으로써, 위 두 서비스용 트래픽 암호화 키를 갱신하는데 있어서 무선 구간 신호 채널의 사용 부하를 현저하게 감소시킬

수 있다. 이에 IEEE 802.16 WirelessMAN 시스템 기반의 무선 인터넷 시스템은 Multicast 서비스나 Broadcast 서비스를 안전하게 끊임없이 제공할 수 있을 뿐만 아니라 신호 채널과 관련된 무선 자원을 보다 효율적으로 사용 가능할 수 있게 되어 전체 시스템하의 성능을 높일 수 있다.

<11> 본 발명이 속하는 기술 분야는 데이터 트래픽의 보안 분야로, 적용 대상이 되는 시스템은 IEEE 802.16 WirelessMAN 시스템이다. IEEE 802.16 WirelessMAN 시스템에서 제공하는 Mulitcast 서비스 또는 Broadcast 서비스용 트래픽 암호화 키를 효율적으로 관리하기 위한 방법에 관한 것이다.

<12> 기존 IEEE 802.16 WirelessMAN 시스템에서는 트래픽 데이터를 암호화하기 위해서 모든 트래픽 암호화 키를 생성하고 분배하는 방식을 정의하였다. 또한, 이 트래픽 암호화 키 또한 보안을 유지하기 위해서 일정 시간이 지나면 갱신하여 새로운 트래픽 암호화 키를 생성 및 분배한다. 이를 통해, 단말과 기지국은 동일한 트래픽 암호화 키를 공유한다. 이와 같이 인증 및 보안 관련 기능을 수행하기 위해서, 단말과 기지국은 PKM-REQ (Privacy Key Management Request) 메시지와 PKM-RSP (Privacy Key Management Response) 메시지를 사용한다. 단말은 PKM-REQ 메시지 중 한 메시지인 Key Request 메시지를 기지국으로 전송함으로써 새로운 트래픽 암호화 키에 대한 할당을 요구하거나 트래픽 암호화 키 갱신을 요구한다. 이 메시지를 수신한 기지국은 응답으로서 트래픽 암호화 키 할당이나 갱신이 성공하였을 경우에는 PKM-RSP 메시지 중 한 메시지인 Key Reply 메시지를, 실패하였을 경우에는 Key Reject 메시지를 해당 단말로 전송한다. 이와 같은 일련의 트래픽 암호화 키 할당

및 갱신 절차를 통해 단말과 기지국 사이에서 공유하게 된 트래픽 암호화 키를 이용하여 무선 구간의 트래픽 데이터를 암호화 및 복호화하여 송, 수신하게 된다.

<13> IEEE 802.16 WirelessMAN 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 방법은 Unicast 서비스용 트래픽 암호화 키 갱신 방법과 동일하다. 하지만, Unicast 서비스용 트래픽 암호화 키 갱신 방법과 동일한 절차로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하는 것은 무선 채널 자원을 불필요하게 사용하는 제한점이 있다. 이에 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신에 따른 무선 채널 자원을 효과적으로 감소하는 절차가 필요하다.

【발명이 이루고자 하는 기술적 과제】

<14> 본 발명은 상기에 기술한 바와 같이, IEEE 802.16 WirelessMAN 시스템에서 기존에 정의하였던 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하기 위해 사용되는 신호 메시지의 무선 채널 구간에서 불필요한 사용을 줄이기 위해서 새로운 갱신 방법을 제안하고자 한다. 즉, 이 발명의 궁극적인 목적은 Multicast 서비스나 Broadcast 서비스용 트래픽 데이터를 끊임없이 안전하게 전달하기 위해 이런 서비스들의 트래픽 암호화 키를 주기적으로 갱신하는데, 이와 같이 트래픽 암호화 키를 갱신할 때 사용되는 메시지를 방송 신호 채널을 사용하여 전달함으로써 기존 방식보다 훨씬 적은 양의 신호 무선 자원으로도 효과적으로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 분배하기 위함이다.

【발명의 구성】

<15> 제 1도는 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 생성, 분배 및 갱신하는 절차도이다.

<16> IEEE 802.16 WirelessMAN 시스템에서 단말 (SS, 101)은 임의의 Multicast 서비스나 Braodcast 서비스를 받기 전에 우선 해당 트래픽 데이터를 암호화는데 필요한 트래픽 암호화 키를 분배받아야 한다. 여기에서 모든 Multicast 서비스나 Broadcast 서비스에는 각각의 서비스 트래픽 데이터를 암호화하기 위해 개별적인 트래픽 암호화 키가 존재한다. 다시 말해서, 모든 Multicast 서비스용 트래픽 암호화 키가 서로 다르고 Broadcast 서비스용 트래픽 암호화 키와도 다르기 때문에, 하나의 트래픽 암호화 키를 단말이 안다고 할지라고 다른 Multicast 서비스를 제공받을 수 없는 것이다.

<17> 트래픽 암호화 키, 트래픽 암호화 키 일련번호, 트래픽 암호화 키 유효시간, 암호화 알고리즘 등을 포함하는 집합을 하나의 SA (Security Association)으로 표현한다. 이 SA에는 식별자 기능을 하는 SA-ID도 포함하고 있다. Multicast 서비스나 Broadcast 서비스는 서로 다른 하나의 SA와 관련되어 있다. 다시 말해서, 임의의 동일한 Multicast 서비스를 제공받는 단말들은 동일한 하나의 SA 정보를 가지고 있고 Broadcast 서비스를 제공받는 단말들도 동일한 하나의 SA 정보를 가지고 있지만, 이 들 Multicast 서비스나 Broadcast 서비스와 관련된 SA가 서로 독립적이기 때문에 이들 개별 서비스 하나당 하나의 SA와 관련있다고 간주할 수 있다.

<18> 단말이 전송하는 해당 서비스의 트래픽 암호화 키 분배 요청 메시지의 MAC

헤더에는 Primary Management CID가 사용된다. Primary Management CID는 기지국이 단말의 초기 접속시 단말마다 고유하게 할당해주는 CID로써 단말을 구별해줄 수 있다. 이 Key Request 메시지에는 해당 서비스와 관련된 SA의 식별자인 SA-ID가 포함되어 있어서 그림 예에서와 같이 n번째 SA 즉 트래픽 암호화 키와 그에 따른 정보들을 요청하는 것이다.

<19> 이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 생성 및 분배 요청 메시지인 Key Request 메시지를 수신한 기지국은 해당 서비스용으로 기존에 생성하였던 트래픽 암호화 키를 요청하였던 단말로 Key Reply 메시지를 통해 전송한다 (S112). 단말이 n번째 SA를 요구하였기 때문에 기지국은 n번째 SA들을 응답 메시지인 Key Reply 메시지에 포함시켜 전송하는 것이다. 이 때의 Key Reply 메시지의 MAC 헤더에는 트래픽 암호화 키를 요청하였던 단말에게만 전송해야 하므로 Key Request 메시지의 MAC 헤더에 포함되었던 Primary Management CID를 그대로 사용한다. 이로써 단말이 임의의 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 최초로 분배받는 절차가 완료되는 것이다.

<20> Key Reply 메시지를 통해 수신한 n번째 SA의 기지국이 x번째로 생성한 트래픽 암호화 키를 가지고 단말은 해당 서비스의 트래픽 데이터를 복호화하는 것이다. 또한, x번째로 생성된 트래픽 암호화 키를 Key Reply 메시지로 분배 받자마자 해당 트래픽 암호화 키의 실제 유효 시간이 시작된다 (111). 이 후 단말은 끊임없이 안전하게 트래픽 서비스를 제공받기 위해서 주기적으로 트래픽 암호화 키를 갱신해야 한다. 이를 위해 단말은 내부적으로 TEK Grace Time (112)을 관리한다. 이 TEK

Grace Time은 이전에 할당 받았던 트래픽 암호화 키가 만료되기 전에 단말이 트래픽 암호화 키 갱신 요청을 유발하는 시점을 의미한다. 즉, 단말은 이 TEK Grace Time이 작동하게 되면 트래픽 암호화 키 상태 머신으로 TEK Refresh Timeout (S121) 이벤트를 발생시킨다.

<21> TEK Refresh Timeout 이벤트로 인해 단말은 기지국으로 트래픽 암호화 키 갱신 및 분배 요청 메시지인 Key Request (S131) 메시지를 전송한다. Key Request 메시지의 MAC 헤더에는 최초로 트래픽 암호화 키를 요청하였던 Key Request 메시지 (S111)의 MAC 헤더에서 포함되었던 Primary Management CID를 사용한다. Key Request 메시지에는 해당 Multicast 서비스나 Broadcast 서비스에 관련된 SA (Security Association)의 식별자 (SA-ID)가 포함되어 있다. n번째 SA에서 새로운 트래픽 암호화 키를 요구하기 때문에 Key Request 메시지에 포함된 SA-ID값은 n이다.

<22> Key Reuqest 메시지를 수신한 기지국은 응답 메시지로써 트래픽 암호화 키를 생성하고 이 트래픽 암호화 키를 Key Reply 메시지에 포함시켜 해당 단말로 전송한다 (S132). Key Reply 메시지의 MAC 헤더에도 트래픽 암호화 키를 최초로 분배하였던 Key Reply 메시지 (S112)의 MAC 헤더에서 사용하였던 Primary Management CID를 사용한다. Key Request 메시지에 SA-ID값이 n이기 때문에 Key Reply 메시지에는 n번째의 SA가 포함된다. 이 SA에는 기지국이 x+1번째로 생성한 트래픽 암호화 키가 존재한다. 단말이 x+1번째로 생성된 트래픽 암호화 키를 Key Reply 메시지로 분배받자마자 해당 x+1번째의 트래픽 암호화 키 실제 유효 시간이 시작된다 (113). 이

후부터 제공받은 해당 서비스 데이터는 x+1번째의 트래픽 암호화 키를 가지고 복호화하는 것이다. 이로써, Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 분배하는 절차가 완료되는 것이다.

<23> IEEE 802.16 WirelessMAN 시스템에서 지원하는 트래픽 암호화 키를 갱신하기 위해서 32바이트의 Key Request 메시지와 74바이트의 Key Reply 메시지가 사용되고 즉, 총 106바이트의 신호 메시지가 사용된다.

<24> 또한, Key Reply 메시지 (S112, S132)에 포함된 트래픽 암호화 키는3-DES알고리즘 방식이 사용되어 암호화되어 있다.

<25> 제 2도는 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 갱신 및 분배하는 방법에 관한 그림이다.

<26> 여기에 도시된 단말들은 하나의 동일한 Multicast 서비스나 Broadcast 서비스를 현재 제공받고 있는 단말들이다. 하나의 Multicast 서비스나 Broadcast 서비스가 n번째 SA와 관련되어 있다고 가정한다. 모든 단말들 (SS1 ~ SSz)은 각각 내부적으로 저장하고 있는 TEK Grace Time에 의해 TEK Refresh Timeout 이벤트가 발생하고 n번째 SA의 트래픽 암호화 키를 갱신받기 위해서 Key Request 메시지를 기지국으로 전송한다 (S211, S221, S231, S2z1). 모든 단말들의 n번째 SA에 해당하는 TEK Grace Time 시점이 동일하기 때문에 모든 단말로부터의 Key Request 메시지들이 거의 한 순간에 기지국으로 전송된다. 이 때 모든 단말들이 Key Request 메시지에는 값이 n인 SA-ID를 포함한다. 하지만, 이 Key Request 메시지의 MAC 헤더에는 단말이 초기 접속 시 기지국으로부터 단말마다 고유하게 할당받은 서로 다른

Primary Management CID가 사용된다. 이처럼 z개의 단말이 현재 서비스를 받고 있는 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 요청 메시지를 전송하기 위해서 동일한 시간에 무선 채널 구간에 하나의 서비스당 32 ? z 바이트가 사용된다.

<27> z개의 단말로부터 n번째 SA의 트래픽 암호화 키 갱신 요청 메시지를 각각 수신받은 기지국은 n번째 SA의 트래픽 암호화 키를 갱신하고 응답 메시지로써 n번째 SA가 포함된 Key Reply 메시지를 모든 단말들에게 동시에 각각 전송한다 (S212, S222, S232, S2z2). 이 때 전송하는 Key Reply 메시지의 MAC 헤더에는 각각의 단말에게 할당된 Primary Management CID가 사용된다. 기지국은 특정 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 분배하기 위해서는 모든 단말에게 일일이 Key Reply 메시지를 전송해야 하기 때문에 무선 채널 구간에 74 ? z 바이트가 사용된다.

<28> 다시 말해서, 특정 Multicast 서비스나 Broadcast 서비스를 제공 받는 모든 단말들은 동일한 하나의 트래픽 암호화 키를 기지국으로부터 분배받아 해당 서비스 트래픽 데이터를 복호화할 때 사용한다. 하지만, 동일한 트래픽 암호화 키를 갱신하는데 있어서 모든 단말이 갱신 요청을 하고 이에 따라 기지국이 모든 단말에게 일일이 갱신된 트래픽 암호화 키를 분배하는 방식은 비효율적이다. 예를 들면, 하나의 Multicast 서비스나 Broadcast 서비스를 제공받고 있는 단말이 z개라면 해당 서비스용 트래픽 암호화 키를 갱신하는데 총 106 ? z 바이트가 필요하다. 이는 무선 채널의 신호 자원의 과다한 낭비이다.

<29> 즉, 이처럼 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하는데 있어서, Unicast 서비스용 트래픽 암호화 키를 갱신하는 방법처럼 모든 단말이 해당 서비스의 트래픽 암호화 키 갱신을 유발하여 요청하고, 이 요청에 대하여 기지국이 모든 단말에게 분배하는 것은 임의의 짧은 순간에 무선 채널의 신호 자원을 낭비하고 기지국의 불필요한 처리량을 야기한다.

<30> 제 3도는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신하기 위한 암호 관련 PKM 파라미터 테이블이다 (300).

<31> 여기에서 M&B (Multicast & Broadcast) TEK Grace Time은 기지국이 내부적으로 저장하고 있는 파라미터로써 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키가 만료되기 전 기지국이 해당 서비스의 트래픽 암호화 키를 갱신을 시작하는 시점을 의미한다. 이 M&B TEK Grace Time은 단말이 트래픽 암호화 키가 만료되기 전 갱신을 시작하는 시점을 의미하는 TEK Grace Time보다 큰 값을 가져야한다. 왜냐하면, Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키 갱신을 단말이 아닌 기지국이 먼저 시작해야 하기 때문이다.

<32> 제 4도는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 생성, 분배 및 갱신하는 절차도이다.

<33> 단말이 임의의 Multicast 서비스나 Broadcast 서비스를 받기 전에 우선 해당 서비스 트래픽 데이터를 복호하는데 필요한 트래픽 암호화 키를 분배받아야 한다. 이와 같은 최초로 해당 서비스의 트래픽 암호화 키를 분배받는 절차 (S411, S412)는 제 1도에서 단말의 최초 트래픽 암호화 키 분배 절차 (S111, S112)와 동일하다.

<34> n번째 SA의 기지국이 x번째로 생성한 해당 서비스의 트래픽 암호화 키가 포함된 Key Reply 메시지를 단말이 수신받음으로써, x번째의 트래픽 암호화 키의 실제 유효 시간이 시작되고 (411), 이 유효 시간동안 단말은 해당 서비스를 제공받을 때 x번째 트래픽 암호화 키를 가지고 트래픽 데이터를 복호한다.

<35> 해당 서비스의 트래픽 데이터를 끊임없이 안전하게 기지국이 단말에게 제공하기 위해서 n번째 SA의 트래픽 암호화 키를 주기적으로 갱신해야 한다. 하지만, 제 1도에서의 IEEE 802.16 WirelessMAN 시스템에서처럼 단말이 트래픽 암호화 키 갱신을 유발하지 않고, 본 발명에서 제안하는 바는 기지국이 해당 서비스 트래픽 암호화 키를 주기적으로 갱신하는 것이다. 이를 위해 기지국은 내부적으로 제 3도에서 언급하였던 M&B TEK Grace Time 파라미터를 관리하고 있는데, Multicast 서비스나 Broadcast 서비스별로 이 M&B TEK Grace Time (412)시점이 되면 해당 서비스 트래픽 암호화 키 상태 머신으로 M&B TEK Refresh Timeout 이벤트를 발생시킨다 (S421). 이 M&B TEK Refresh Timeout 이벤트로 인해 트래픽 암호화 키 상태 머신에게 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 새롭게 갱신하게 된다.

<36> 기지국은 단말에게 n번째 SA의 갱신된 x+1번째 트래픽 암호화 키를 포함한 Key Reply 메시지를 전송한다 (S431). 단말이 x+1번째로 생성된 트래픽 암호화 키를 Key Reply 메시지로 분배 받자마자 해당 x+1번째의 트래픽 암호화 키 실제 유효 시간이 시작된다 (413). 이 후부터 제공받은 해당 서비스 데이터는 x+1번째의 트래픽 암호화 키를 가지고 복호화하는 것이다.

<37> Key Reply 메시지의 MAC 헤더에는 Broadcast CID가 사용함으로써, 한 번의 Key Reply 메시지로 모든 단말에게 갱신된 트래픽 암호화 키를 Broadcast Connection을 통해 효율적으로 분배하는 것이다. 특히, Broadcast Connection을 통해 전송하는 Key Reply 메시지에 포함된 트래픽 암호화 키가 어떠한 Multicast 서비스 데이터를 암호화하는데 필요한 트래픽 암호화 키인지 또는 Broadcast 서비스 데이터를 암호화하는데 필요한 트래픽 암호화 키인지를 구별해야 하는데, 이는 Key Reply 메시지에 포함된 SA의 식별자인 SA-ID로 구별한다. 그림 4에서 갱신하여 분배하는 Key Reply 메시지에 포함된 x+1번째 트래픽 암호화 키는 n번째 SA로써 이 SA와 관련된 서비스를 암호화하는데 사용됨을 알 수 있다.

<38> Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 기지국이 자체적으로갱신하는 방식에서 사용되는 Key Reply 메시지는 74바이트로써, Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하여 모든 단말에게 분배하는데 필요한 메시지 양은 총 74바이트이다.

<39> 만약, 해당 서비스에 대하여 단말이 관리하는 TEK Grace Time 시점까지 기지국으로부터 Broadcast Connection을 통해 트래픽 암호화 키를 갱신 및 분배하는 Key Reply 메시지를 단말이 수신하지 못하였다면, 단말의 TEK Grace Time 시점에 해당 서비스의 트래픽 암호화 키 상태 머신에 그림 1과 같이 TEK Refresh Timeout 이벤트가 발생한다 (S121). 이 후 단말은 트래픽 암호화 키 갱신 및 분배 요청 메시지인 Key Request 메시지를 Primary Management Connection을 통해 전송하고 (S131), 이에 대한 응답 메시지로 기지국은 단말에게 갱신된 트래픽 암호화 키가

포함된 Key Reply 메시지를 Primary Management Connection을 통해 전송한다 (S132). 즉, 단말이 기지국으로부터 새로운 트래픽 암호화 키를 TEK Grace Time 시점까지 분배받지 못하면 그림 1에서처럼 단말이 해당 서비스에 대한 트래픽 암호화 키 갱신을 시작하는 방식의 절차를 수행하게 된다.

<40> 제 5도는 본 발명에서 제안하는 Mutlicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 분배하는 방법에 관한 그림이다.

<41> 여기에 도시된 단말들은 하나의 동일한 Multicast 서비스나 Broadcast 서비스를 현재 제공받고 있는 단말들이다 (SS1 ~ SSz). 하나의 Multicast 서비스나 Broadcast 서비스가 n번째 SA와 관련되어 있다고 가정한다. 기지국은 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 자체적으로 갱신하기 위해서 내부적으로 그림 3에서 언급한 바와 같이 M&B TEK Grace Time을 관리하고 있는데, 이 M&B TEK Grace Time 시점에 M&B TEK Refresh Timeout 이벤트를 발생한다.

<42> M&B TEK Refresh Timeout 이벤트로 인해 기지국은 해당 서비스용 트래픽 암호화 키를 갱신하고 이를 모든 단말들에게 하나의 Key Reply 메시지를 Broadcast Connection을 통해 전송함으로써 트래픽 암호화 키를 분배한다 (S511, S521, S531, S5z1). 즉, 이 때 전송하는 Key Reply 메시지의 MAC 헤더에는 모든 단말들에게 한번에 전달할 수 있는 Broadcast CID가 사용된다.

<43> 따라서, 본 발명이 제안한 방식에서 기지국이 특정 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 모든 단말들에게 분배하기 위해서 무선 채널 구간에서 사용되는 신호 자원은 총 74바이트에 불과하다. 이에 비해, 단

말이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신을 시작하는 방식에서는 z개의 단말이 트래픽 암호화 키를 갱신하는데 총 106 ? z 바이트의 신호 자원이 필요하며 이는 비효율적이다. 또한, 기지국 입장에서 볼 때, 단말이 트래픽 암호화 키 갱신을 시작하는 방식에서는 한 순간에 MAC 메시지와 해당 SA를 생성하는데 너무나 많은 처리량이 필요하지만, 본 발명에서 제안하는 방식은 작은 처리량으로도 해당 Multicast 서비스나 Broadcast 서비스를 제공받고 있는 단말들에게 트래픽 암호화 키를 안정적으로 갱신 및 분배할 수 있다는 장점이 있다.

<44> 제 6도는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 분배시 MAC 헤더의 CID값과 이에 따른 트래픽 암호화 키를 암호화하는 입력 키간의 관계를 설명해 주는 테이블이다.

<45> 제 7도는 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 갱신된 트래픽 암호화 키를 분배하는 방식에서의 모든 서비스에 대한 트래픽 암호화 키 상태 머신 흐름에 대한 그림이다 (700).

<46> 단말은 Unicast 서비스, Multicast 서비스 또는 Broadcast 서비스와 상관없이 모든 서비스에 대하여 트래픽 암호화 키 상태 머신 흐름도의 흐름을 따르고 최대 두 개씩의 트래픽 암호화 키 상태 머신이 존재한다.

<47> 단말이 Multicast 서비스나 Broadcast 서비스를 제공받고자 할 때 해당 서비스에 대한 트래픽 암호화 키를 기지국으로 요청하고 기지국으로부터 이를 분배받는다 (S411, S412). 이와 같은 절차를 통해 단말은 해당 서비스용 트래픽 암호화 키를 기지국과 공유하게 되어 트래픽 암호화 키 상태 머신이 "Operational" 상태에 있게

된다. 일정 시간 후 해당 서비스에 대하여 기지국이 트래픽 암호화 키를 자체적으로 갱신을 시작하고 (S421) 갱신된 트래픽 암호화 키를 단말로 전송한다 (S431). 기존의 유효한 트래픽 암호화 키를 가지고 "Operational" 상태에 있는 단말이 해당 서비스에 대한 갱신된 트래픽 암호화 키가 포함된 Key Reply 메시지를 받게 되면, 인증 및 보안과 관련된 자체 데이터베이스에 새로이 갱신된 SA를 저장하고 다시 "Operational" 상태에 머무르게 된다.

<48> 제 8도는 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 갱신된 트래픽 암호화 키를 분배하는 방식에서의 모든 서비스에 대한 트래픽 암호화 키 상태 천이를 나타내는 테이블이다 (800).

<49> 이는 서비스에 대한 트래픽 암호화 키 상태 흐름도 (700)를 테이블로 나타낸 것이다. 여기에서, 8-D 구간에 표시된 것은 오직 Multicast 서비스나 Broadcast 서비스에 한해서만 규정된 것이다. Multicast 서비스나 Broadcast 서비스를 제공받은 단말이 이미 해당 서비스용 트래픽 암호화 키를 분배받아서 내부적으로 관리하고 있는 트래픽 암호화 키 상태 머신이 "Operational" 상태일 때, 기지국으로부터 해당 서비스용 트래픽 암호화 키를 Key Reply를 통해 새로이 분배받으므로써 다시 "Operational" 상태에 머물게 된다.

<50> 본 발명에서는 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 단말이 분배받을 때에 있어서 두 가지 방법으로 정의할 수 있다. 하나는 단말이 임의의 Multicast 서비스나 Broadcast 서비스를 제공받기 위해 해당 서비스용 트래픽 암호화 키 분배를 요청하는 절차와 또 다른 하나는 이 후 기지국이 해당 서비스를

제공받고 있는 단말들에게 일률적으로 해당 트래픽 암호화 키를 갱신하여 분배하는 절차가 있다. 기지국으로부터 분배되는 트래픽 암호화 키는 두 개의 입력키를 사용하는 3-DES 방식의 알고리즘을 이용하여 암호화되어 단말에게 전달된다. 암호화된 트래픽 암호화 키를 수신한 단말은 미리 공유한 두 개의 입력키를 사용하여 복호해서 실제적인 트래픽 암호화 키를 갖게 되는 것이다. 트래픽 암호화 키의 지속적인 보안을 유지하기 위해서 단말의 요청에 따른 트래픽 암호화 키 갱신 절차와 기지국의 자체적인 트래픽 암호화 키 갱신 절차에 따라 트래픽 암호화 키를 암호화하는 두 개의 입력키들이 달라진다.

<51> 첫째, 단말이 해당 서비스의 트래픽 암호화 키에 대한 분배를 요청할 때에는 단말Key Request 메시지를 전송하고 기지국은 이에 대한 응답 메시지로써 갱신된 트래픽 암호화 키를 포함한 Key Reply 메시지를 단말로 전송한다 (S411, S412). 이 경우 Key Request 메시지와 Key Reply 메시지는 기지국과 하나의 단말과의 교환을 하기 때문에 MAC 헤더에 Primary Management CID를 사용한다. 즉, 단말의 사유 채널인 Primary Management Connection을 통해 수신 받은 트래픽 암호화 키는 해당 단말과 기지국만이 알고 있는 사유키 (Private Key)를 통해 암호화되어 있다. 이 때 사유키는 해당 단말의 인증키로부터 만들어진 KEK (Key Encryption Key)를 사용한다. 128비트인 KEK를 64비트로 나누어서 상위 64비트의 KEK와 하위 64비트의 KEK가 Primary Management CID를 사용하여 분배되는 트래픽 암호화 키를 3-DES 방식의 알고리즘으로 암호화하는데 있어서 두 개의 입력키가 되는 것이다.

<52> 둘째, 기지국이 자체적으로 트래픽 암호화 키를 갱신하고 단말들에게 일률적

으로 분배하는 절차에 있어서 Key Reply 메시지를 이용하여 트래픽 암호화 키를 전송한다 (S431). 이 경우 Key Reply 메시지는 기지국에서 해당 서비스를 제공 받고 있는 모든 단말들에게 전송해야 하기 때문에 MAC 헤더에 Broadcast CID를 사용한다. 해당 서비스의 트래픽 암호화 키를 Broadcast Connection을 통해 전송하기 때문에 기지국과 단말 사이의 사유키를 가지고 이 트래픽 암호화 키를 암호화할 수 없다. 그러므로, 이 경우에 있어서 사유키를 사용하지 않고 기지국과 해당 서비스를 제공받고 있는 모든 단말 사이의 공용키를 가지고 트래픽 암호화 키를 암호화하여 분배해야 한다. 하지만, 이 공용키는 Multicast 서비스마다 또한 Broadcast 서비스에서만 고유하고 보안을 유지할 수 있는 키이어야한다. 해당 서비스 트래픽 데이터 암호용으로 사용하였던 이전에 분배받았던 트래픽 암호화 키는 이러한 특성을 가지고 있는 공용키이다. Multicast 서비스마다 또한 Broadcast 서비스에서만 개별적인 이전에 분배받았던 64비트의 트래픽 암호화 키가 Broadcast CID를 사용하여 분배되는 트래픽 암호화 키를 3-DES 방식의 알고리즘으로 암호화하는데 있어서 입력키가 된다. 두 개의 입력키는 이전에 분배받았던 64비트의 트래픽 암호화 키가 두 번 사용되는 것이다.

<53> 따라서, 기지국은 단말의 요청으로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 및 분배할 때 갱신된 트래픽 암호화 키는 KEK를 입력으로 하여 암호화하고 이를 Primary Management CID를 사용하여 단말에게 전송하고, 기지국 자체적으로 해당 서비스용 트래픽 암호화 키 갱신 및 분배할 때에는 갱신된 트래픽 암호화 키는 이전에 해당 서비스용으로 생성하였던 트래픽 암호화 키를 입

력으로 하여 암호화하여 이를 Broacast CID를 사용하여 모든 단말에게 전송한다. 또한, 단말은 Primary Management CID를 사용한 Key Reply 메시지를 통해 트래픽 암호화 키를 전달받았다면 KEK를 이용하여 트래픽 암호화 키를 복호하고, Broadcast CID를 사용한 Key Reply 메시지를 통해 트래픽 암호화 키를 전달받았다면 해당 서비스용으로 이전에 분배받았던 트래픽 암호화 키를 이용하여 트래픽 암호화 키를 복호하는 것이다. 이로써, 트래픽 암호화 키조차도 계속적으로 보안을 유지하고 Broadcast Connection을 통해 트래픽 암호화 키를 분배받음으로써 시스템 전체적으로 효율적으로 운영할 수 있다.

【발명의 효과】

<54> 본 발명은 IEEE 802.16 WirelessMAN 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 관리하는 메커니즘을 정의하는 것으로, 다음과 같은 효과가 있다.

<55> 첫째, Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 갱신을 기지국이시작하여 갱신된 키를 해당 서비스를 제공받는 단말들에게 Broadcast Connection을 통해 전달함으로써, 적은 신호 자원을 가지고도 트래픽 암호화 키를 갱신 및 분배가 가능하다.

<56> 둘째, 기지국이 상기 서비스들의 트래픽 암호화 키를 갱신하고 단말에게 일률적으로 분배하는 방식을 사용함으로써, 단말로부터 일시적인 트래픽 암호화 키 요청 메시지를 사용하지 않고 하나의 Key Reply 메시지로 모든 단말에게 트래픽 암호화 키를 분배하게 되어 기지국 입장에서 이러한 트래픽 암호화 키와 관련된 처리

량이 감소된다는 장점이 있다.

<57> 셋째, Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 기지국에서 주기적으로 갱신함으로써 상기 서비스에 대한 강력한 보안을 유지하면서 단말에게 서비스를 제공할 수 있다.

<58> 넷째, Multicast 서비스의 경우 Multicast 서비스마다 관련된 SA 특히 트래픽 암호화 키가 다르므로 Multicast 서비스마다 보안 유지가 가능하다.

【특허청구범위】

【청구항 1】

IEEE 802.16 WirelessMAN 기반의 무선 인터넷 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 및 분배하는 방법.

【청구항 2】

제 1항에 있어서, 기지국이 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키 갱신을 시작하는 방법

【청구항 3】

제 2항에 있어서, Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키가 만료되기 전 기지국이 트래픽 암호화 키 갱신을 시작하는 시간인 M&B TEK Grace Time을 사용하는 방법.

【청구항 4】

제 3항에 있어서, 기지국의 M&B TEK Grace Time 값이 단말의 TEK Grace Time 값보다 큰 값으로 설정함으로써, 단말이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키에 대하 갱신을 시작하기 전에 기지국이 먼저 시작하는 방법.

【청구항 5】

제 3항에 있어서, 기지국에 설정된 M&B TEK Grace Time으로 인해 트래픽 암호화 키 상태 머신에 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 요청 이벤트인 M&B TEK Refresh Timeout 이벤트를 발생시키는 방법.

【청구항 6】

제 1항에 있어서, 임의의 한 가지 Multicast 서비스나 Broadcast 서비스를 제공받고 있는 단말들로부터 트래픽 암호화 키 갱신 요청 메시지를 받기 전에 갱신된 해당 서비스의 트래픽 암호화 키를 기지국이 모든 단말에게 각각 Primary Management Connection이 아닌 Broadcast Connection을 통해 전송하는 방법.

【청구항 7】

제 6항에 있어서, 갱신된 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 기지국이 Broadcast Connection을 통해 분배할 때 PKM 메시지의 한 메시지인 Key Reply 메시지를 이용하는 방법.

【청구항 8】

제 1항에 있어서, 기지국에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 분배할 때 트래픽 암호화 키 자체도 3-DES 알고리즘 방식을 통해 암호화해서 단말로 전송하는 방법.

【청구항 9】

제 6항 또는 8항에 있어서, 단말이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 요구 시 기지국이 Primary Management Connection을 통해 분배한 트래픽 암호화 키와 기지국 자체적으로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신을 시작하고 Broadcast Connection을 통해 분배한 트래픽 암호화 키는 서로 다른 입력 키를 가지고 암호화하는 방법.

【청구항 10】

제 9항에 있어서, Primary Management Connection을 통해 분배하는 트래픽 암호화 키는 KEK를 사용하여 암호화는 방법.

【청구항 11】

제 9항에 있어서, Broadcast Connection을 통해 분배하는 트래픽 암호화 키는 기존에 분배하였던 해당 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 사용하여 암호화하는 방법.

【청구항 12】

제 11항에 있어서, 기존에 분배하였던 64비트의 트래픽 암호화 키가 3-DES 알고리즘 방식의 두 개 입력키로써 공히 사용되는 방법.

【청구항 13】

제 1항, 제 2항, 제 6항중 어느 하나의 항에 있어서, 단말마다 저장하고 있는 트래픽 암호화 키가 만료되기 전 단말이 트래픽 암호화 키 갱신을 요청하는 시간인 TEK Grace Time까지 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키가 갱신된 메시지를 수신받지 못했을 경우 단말이 해당 서비스용 트래픽 암호화 키 갱신을 시작하는 방법.

【청구항 14】

제 13항에 있어서, 단말은 TEK Grace Time에 내부적으로 트래픽 암호화 키 상태머신에 TEK Refresh Timeout이벤트를 발생시키고 이 이벤트로 인해 기지국으로

트래픽 암호화 키 갱신 및 분배 요청 메시지인 Key Request 메시지를 송신하는 방법.

【청구항 15】

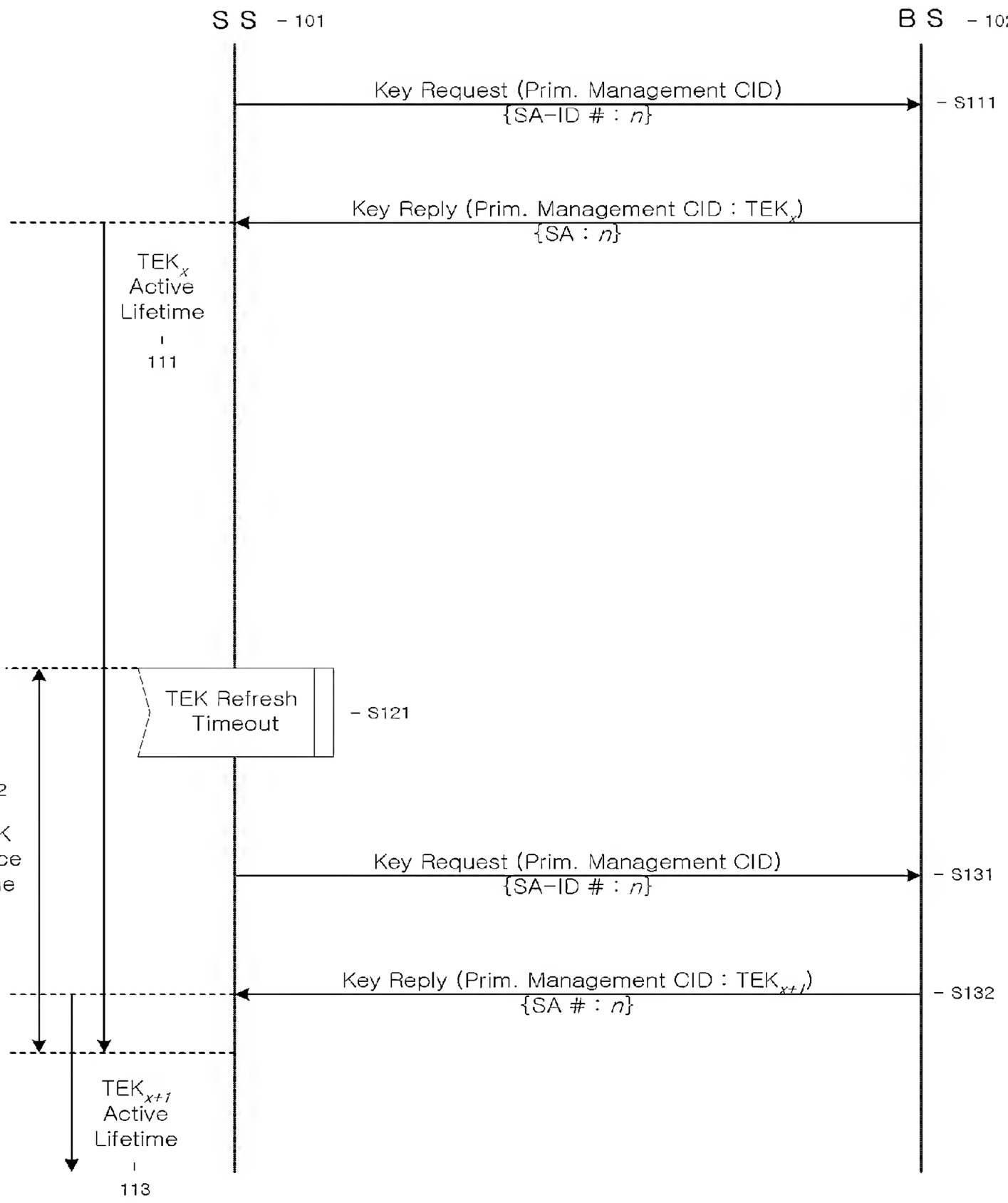
제 14항에 있어서, Key Request 메시지를 수신한 기지국은 해당 서비스의 트래픽암호화 키를 갱신하고 이를 트래픽 암호화 키 갱신을 요청한 단말에게 Key Reply 메시지를 통해 트래픽 암호화 키를 분배하는 방법.

【청구항 16】

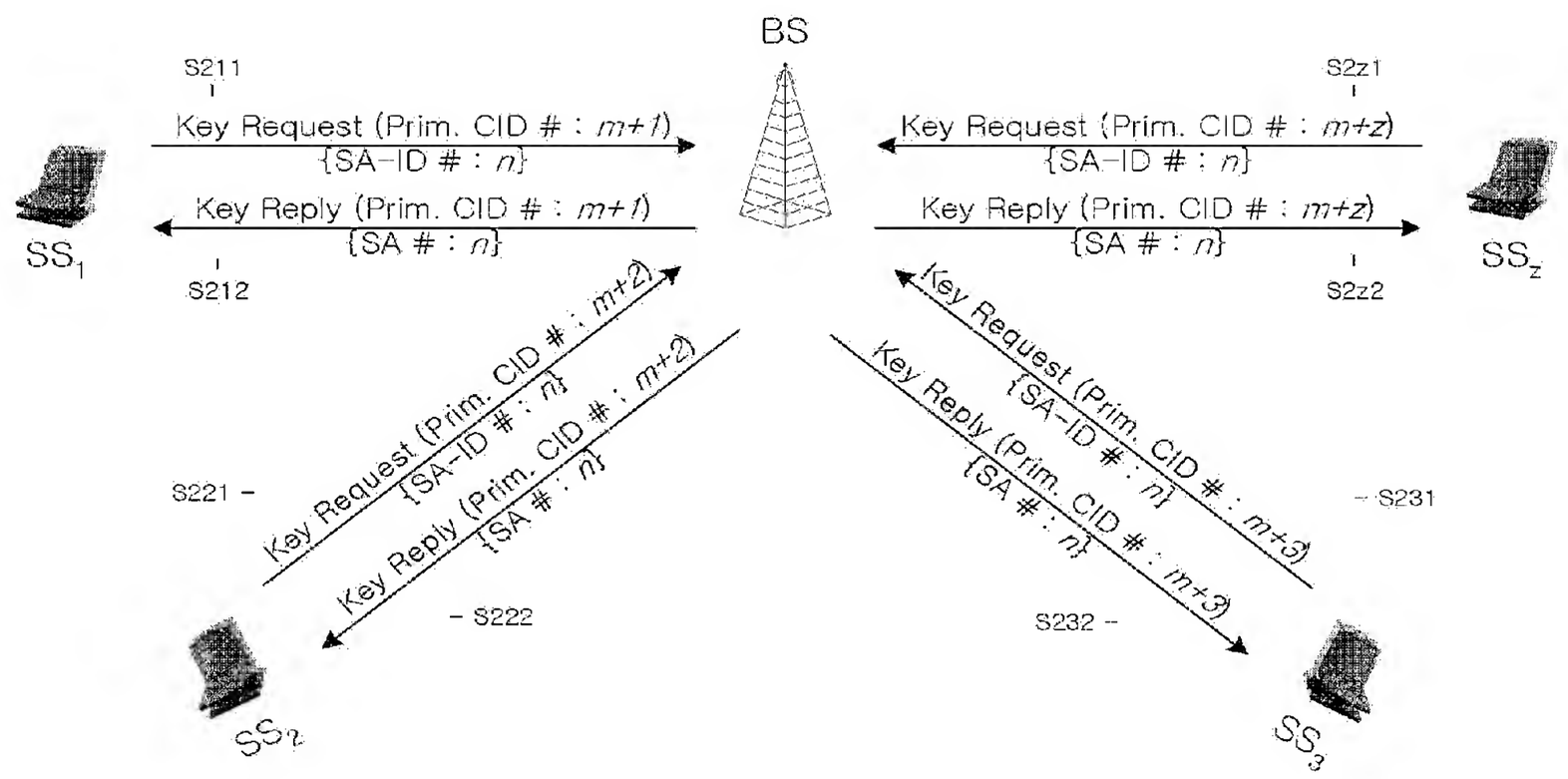
제 1항에 있어서, Multicast 서비스나 Broadcast 서비스는 각각 하나의 독립적이고 고유한 SA에 매핑하는 방법.

【도면】

【도 1】


S S - 101
B S - 102
Key Request (Prim. Management CID)
{SA-ID # : n}
- S111
Key Reply (Prim. Management CID : TEK_x)
{SA : n}
TEK_x Active Lifetime
111
TEK Refresh Timeout
- S121
112
TEK Grace Time
Key Request (Prim. Management CID)
{SA-ID # : n}
- S131
Key Reply (Prim. Management CID : TEK_x+1)
{SA # : n}
- S132
TEK_x+1 Active Lifetime
113

【도 2】

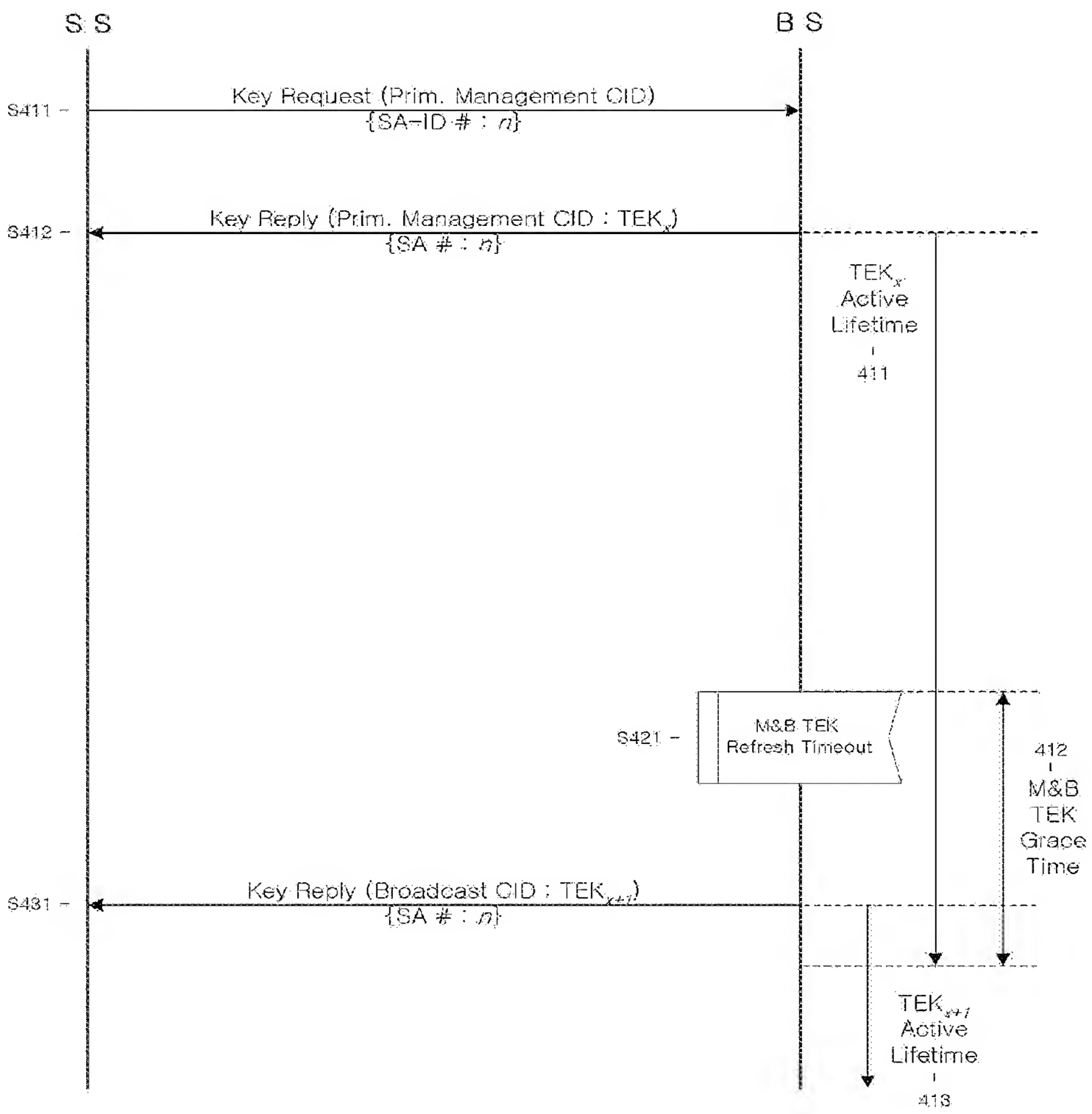


【도 3】

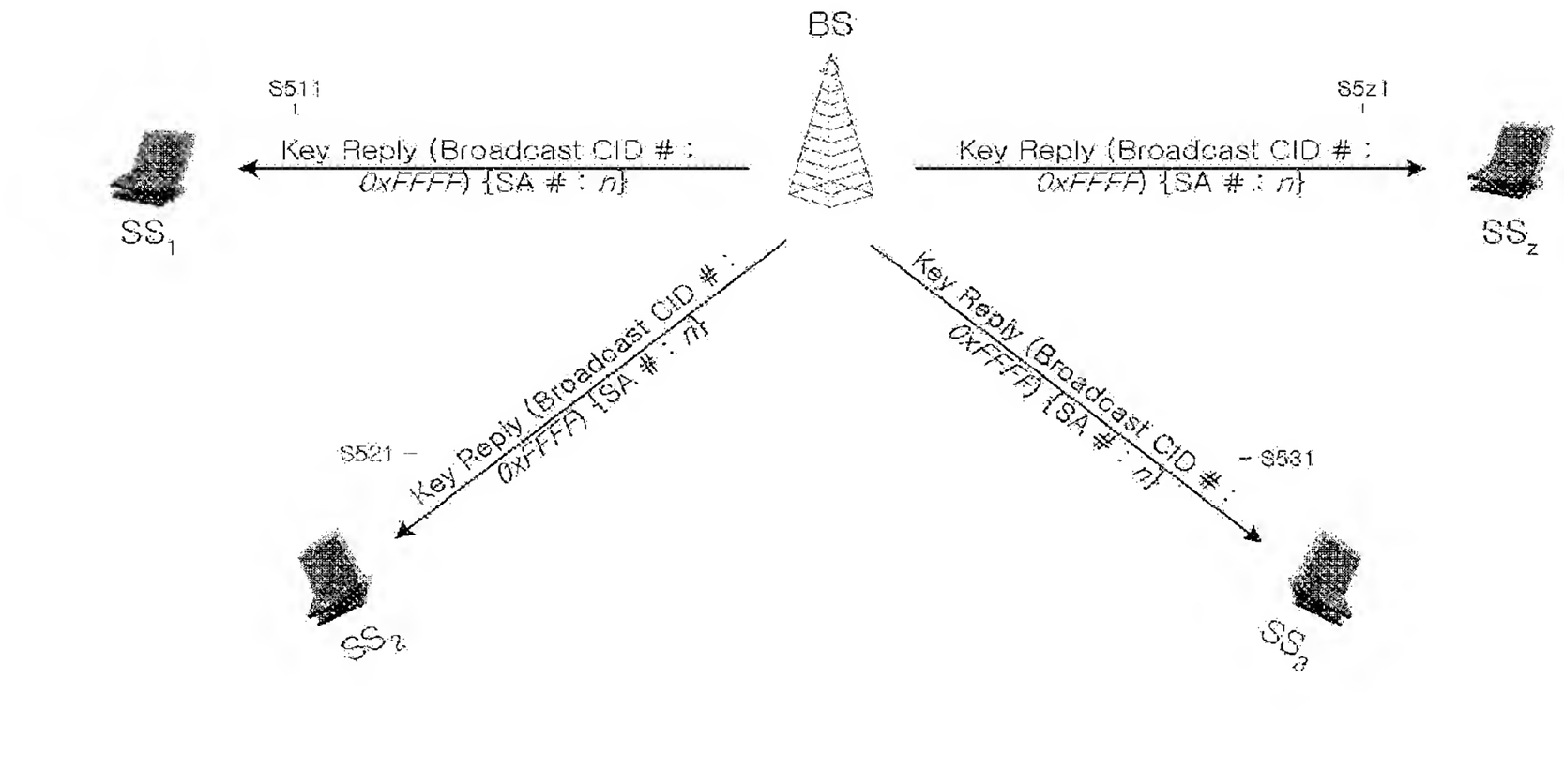
Operational ranges for privacy configuration setting - 300

System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to TEK (for the multicast and broadcast traffic service) expiration BS begins rekeying. This time is longer than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value

【도 4】


S S
B S
S411
Key Request (Prim. Management CID)
{SA-ID # : n}
S412
Key Reply (Prim. Management CID : TEK$_x$)
{SA # : n}
TEK$_x$ Active Lifetime
411
S421
M&B TEK Refresh Timeout
412
M&B TEK Grace Time
S431
Key Reply (Broadcast CID : TEK$_{x+1}$)
{SA # : n}
TEK$_{x+1}$ Active Lifetime
413

【도 5】

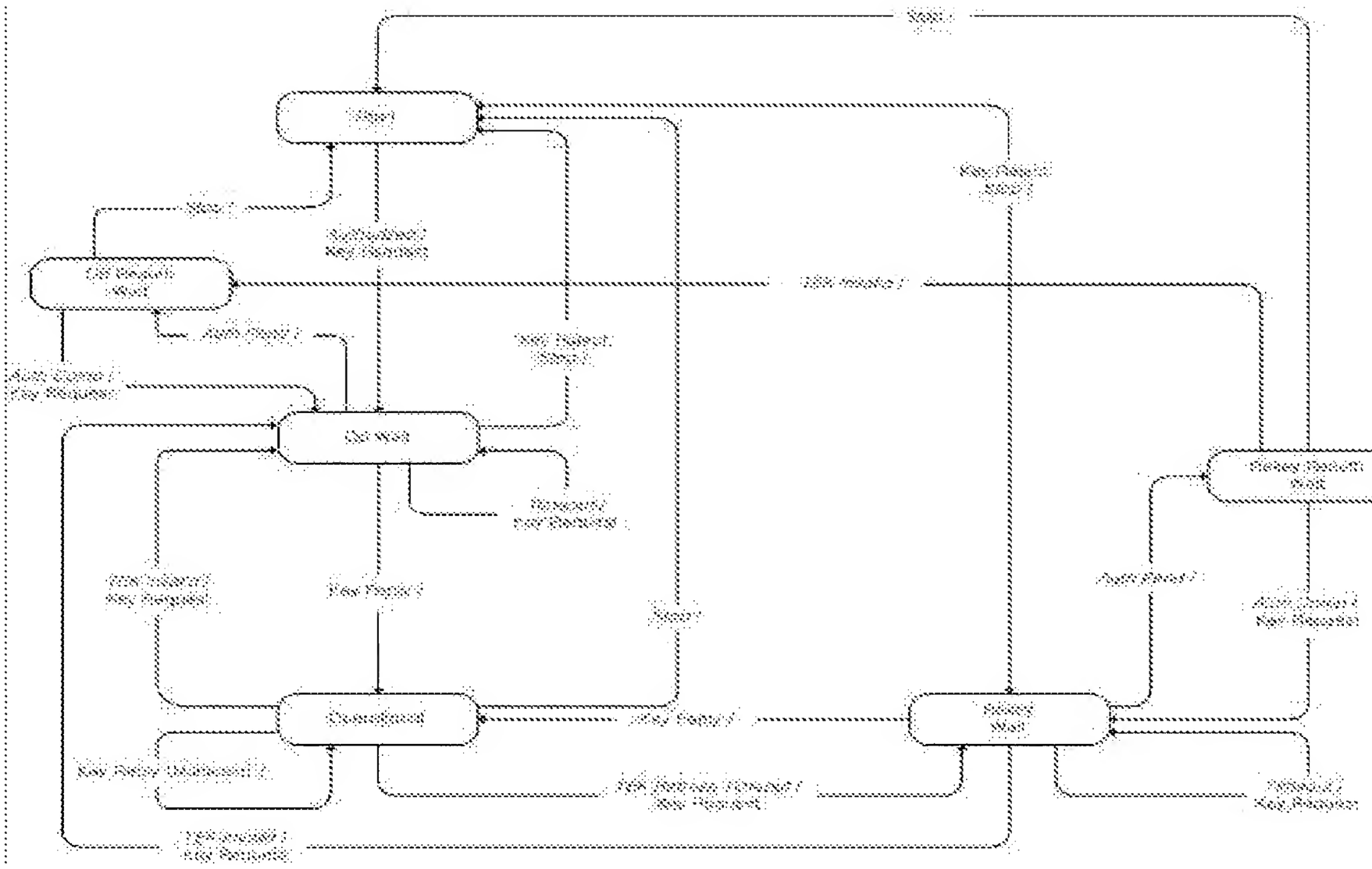


【도 6】

Relationship between the CID and input key used to encrypt the new TEK – 600

CID (MAC Header)	Key to encrypt the TEK
Primary Management CID	KEK (Derived from the AK)
Broadcast CID	Old distributed TEK

【도 7】



【도 8】

TEK FSM state transition matrix

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					
(3) Auth Fwd		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait			Rekey Wait	
(7) TEK Refresh Timeout				Rekey Wait		
(8) Key Reply		Operational		Operational	Operational	
(9) Key Reject		Start			Start	